

U.S. Patent Application Serial No. 09/889,918  
Reply to Office Action dated May 16, 2006

**Remarks:**

Applicants have read and considered the Office Action dated May 16, 2006. Claims 20-26 have been amended. Claims 19 and 28 have been cancelled without prejudice or disclaimer. New claims 29-41 have been added. Claims 20-26 and 29-41 are currently pending.

The specification was objected to as it lacks any mention of "the body of integers modulo  $n$ " that is recited in the claims. The claims have been amended to recite "the ring of integers modulo  $n$ ." Applicants assert that there is support for this term in the specification and Applicants assert that the objection to the specification is overcome.

The claims were objected to for a number of informalities. Claims 20-23 and 25-26 use "x" to represent multiplication. The Action asserts that this is inconsistent with the independent claims and the specification. The claims have been amended so that a proper multiplication "•" is used. Claims 24, 25 and 26 recite "the" process. Claims 24 and 25 have been rewritten in independent form and claim 26 refers to the computer implemented process. Claim 28 has now been cancelled. Applicants assert that the claims overcome the objection.

Claims 19-26 and 28 were rejected under 35 U.S.C. § 112 first paragraph as failing to comply with the written description requirement. The Action asserts that "the body of integers modulo  $n$ " lacks support. The Action notes that there is support for "the ring of integers modulo  $n$ ". The claims have been amended and recite "the ring of integers modulo  $n$ " and Applicants assert that there is proper support.

Claims 19-26 and 28 were rejected under 35 U.S.C. § 112 as being indefinite. The Action asserts that the use of parenthesis renders the claims unclear. The parenthesis have been deleted from the objected to portions. Applicants assert that the indefiniteness rejection has been overcome.

U.S. Patent Application Serial No. 09/889,918  
Reply to Office Action dated May 16, 2006

Claims 19, 25 and 28 were rejected under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter. Claims 19 and 28 have been cancelled. Claim 25 has been amended to recite additional steps and is believed to meet the statutory requirements of 35 U.S.C. § 101.

Claims 19-26 and 28 were provisionally rejected on the grounds of non-statutory obviousness-type double patenting as being unpatentable over claims 19-28 of co-pending Application No. 10/089,626. Applicants assert that the claims of the two applications are patentably distinct from each other. The two systems are trying to solve the equation  $G_i = Q^v \bmod n$  utilizes a mathematical analysis. The analysis of the systems described in the two applications is radically different. The patents recites specific mathematical conditions and such conditions are nontrivial and patentably distinct so that the obviousness-type double patenting rejection is improper. Moreover, Applicants assert that the present invention has priority and that both applications should not be restricted with a Terminal Disclaimer. Moreover, Applicants assert that the remaining issues have been resolved and that the only remaining rejections are a provisional obviousness-type double patenting rejection, the rejection should be withdrawn and this application allowed to issue. See MPEP § 804. Applicants request that the double patenting rejection be withdrawn.

Claims 19-26 and 28 were provisionally rejected on the ground of non-statutory obviousness-type double patenting as being unpatentable over claims 1-20 of co-pending Application No. 09/889,958. Applicants assert that Application No. 09/889,958 has been abandoned and the rejection is moot.

Finally, claims 19-26 and 28 were provisionally rejected on the grounds of non-statutory obviousness-type double patenting as being unpatentable over claims 13-24 of co-pending Application No. 09/869,966. Applicants assert that the claims are patentably distinct. Applicants assert that 09/869,966 is directed to precisely describing how one "obtains" adequate values for keys and describes different steps of calculation for allowing one to obtain such keys.

U.S. Patent Application Serial No. 09/889,918  
Reply to Office Action dated May 16, 2006

The application is directed to patentably distinct subject matter. Applicants assert that the provisional double patenting rejection should be withdrawn for these reasons as well as those discussed above.

Applicants assert that the claims are in condition for allowance. A speedy and favorable action on the merits is hereby solicited. If the Examiner feels that a telephone interview may be helpful in this matter, please contact Applicants' Representative at (612) 336-4728.



Respectfully submitted,

MERCHANT & GOULD P.C.

Dated: 8/16/06

By: 

Gregory A. Sebold  
Reg. No. 33,280  
GAS/km